BRANN & ISAACSON
DAVID W. BERTONI (admitted *pro hac vice*)
dbertoni@brannlaw.com
DAVID SWETNAM-BURLAND (State Bar No. 226216)
dsb@brannlaw.com
EAMONN R.C. HART (admitted *pro hac vice*)
ehart@brannlaw.com
184 Main Street
P.O. Box 3070
Lewiston, ME 04243-3070
Tel.: (207) 786-3566
Fax: (207) 783-9325

LAW OFFICES OF RICHARD PACHTER
RICHARD PACHTER (State Bar No. 120069)
richard@pachterlaw.com
555 University Avenue, Suite 200
Sacramento CA 95825
Tel.: (916) 485-1617
Fax: (916) 379-7838

Attorneys for Defendant NaviStone, Inc.

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

JEREMIAH REVITCH,

Plaintiff;
Counterclaim Defendant,

v.

NAVISTONE, INC.,

Defendant; Counterclaimant.

Case No. 3:18-cv-06827-VC

DEFENDANT NAVISTONE, INC.'S OPPOSITION TO PLAINTIFF'S MOTION FOR SUMMARY JUDGMENT (ECF 168) AND CROSS-MOTION FOR SUMMARY JUDGMENT

Hearing Date: June 10, 2021
Time: 2:00 pm
Judge: Hon. Vince Chhabria

NOTICE OF MOTION

Defendant NaviStone, Inc. ("NaviStone") gives notice to all parties and their counsel of record that on June 10, 2021, at 2:00 PM or such other time as ordered by the Court, pursuant to Fed. R. Civ. P. 56, it will and does move the Court for summary judgment in whole or in part on all claims asserted against it by Plaintiff Jeremiah Revitch ("Plaintiff" or "Revitch") and on its counterclaim against Plaintiff. In support of its motion, NaviStone relies on this notice; the following memorandum of points and authorities; declarations of Larry Kavanagh, Chris Ludwig, Greg Humphreys, Michael Schoen, and David Swetnam-Burland ("2d DSB Dec.") and any supporting exhibits to the same; declarations and other evidence previously submitted to the Court (designated here by ECF number), including by NaviStone, Plaintiff, and New Moosejaw, LLC ("Moosejaw"); the pleadings on file; and any other and further matters and arguments presented to the Court at the time of hearing. By order of the Court, *see* ECF 166, and pursuant to ¶ 39 of the Court's Standing Order for Civil Cases, the following brief also serves as NaviStone's opposition to Plaintiff's motion for summary judgment (ECF 168).

By its motion, NaviStone seeks an order granting its motion for summary judgment in whole or in part on Plaintiff's claims and its counterclaim and denying Plaintiff's motion for summary judgment on Plaintiff's claims and NaviStone's counterclaim.

STATEMENT OF ISSUES

Pursuant to Civ. L.R. 7-4(a)(3), NaviStone identifies the following issues for decision:

1. Whether the Court should grant NaviStone's motion for summary judgment on Plaintiff's claim under Cal. Penal Code § 631 in whole or in part, and deny Plaintiff's motion for summary judgment on the same claim;

2. Whether the Court should grant NaviStone's motion for summary judgment on Plaintiff's claim under Cal. Penal Code § 635 in whole or in part, and deny Plaintiff's motion for summary judgment on the same claim;

3. Whether the Court should grant NaviStone's motion for summary judgment on Plaintiff's common law and California constitutional claims; and

4. Whether the Court should grant NaviStone's motion for summary judgment on its declaratory judgment counterclaim in whole or in part, and deny Plaintiff's motion for summary judgment on the same counterclaim.

Respectfully submitted,

Dated: April 22, 2021

/s/ David Swetnam-Burland
David W. Bertoni *(pro hac vice)*
dbertoni@brannlaw.com
David Swetnam-Burland (226216)
dsb@brannlaw.com
Eamonn R.C. Hart (*pro hac vice*)
ehart@brannlaw.com
BRANN & ISAACSON
184 Main Street, 4th Floor
P.O. Box 3070
Lewiston, ME 04243-3070
Tel.: (207) 786-3566
Fax: (207) 783-9325

Richard Pachter (120069)
richard@pachterlaw.com
LAW OFFICES OF RICHARD PACHTER
555 University Avenue, Suite 200
Sacramento CA 95825
Tel.: (916) 485-1617
Fax: (916) 379-7838

Attorneys for NaviStone, Inc.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

Rules

I. INTRODUCTION

In November 2018, Revitch filed this putative class action lawsuit against NaviStone and Moosejaw alleging that the services NaviStone provided to Moosejaw constituted a wiretap under California criminal law.

Over two years later, the factual record yields one inescapable conclusion: NaviStone's software, far from being an illegal "wiretap," is typical web analytics software like that found on tens of millions of websites, including websites operated by Revitch, his lawyers, his experts, and many organs of federal and state government.[1] By his own admission, Revitch suffered no harm from, was unconcerned about, and himself engaged in the practices of which he now complains. By his own admission, Revitch actively avoids learning about Internet privacy practices. He nonetheless asks the court to impose liability on a theory that sweeps in ordinary communications taking place countless of times each day across the World Wide Web. By its own terms, the California Invasion of Privacy Act ("CIPA") does not encompass these services, and the California legislature has enacted a separate statute covering the activities at issue which *does not* prohibit them.

II. FACTUAL BACKGROUND

A. NaviStone's Services

NaviStone assists online retailers to reach potential customers by postal mail while protecting visitor anonymity. ECF 140-1 (First Declaration of Larry Kavanagh ("1st Kavanagh Dec.")) ¶ 8. NaviStone's processes ensure that neither NaviStone nor any of its clients (in this case, Moosejaw), nor any third-party, can ever associate browsing data with an identifiable individual. *Id*. ¶¶ 8–9, 11, 14–15. In addition, NaviStone requires that its clients comply with consumer

[1]Further allegations that NaviStone scanned Revitch's hard drive, *see* ECF 43, ¶¶ 1-3, 9, 17, 20, 26, 42-46, 86, which allowed certain claims of his Second Amended Complaint ("SAC") to survive a motion to dismiss, *see* ECF 64, have been abandoned because they are untrue.

privacy laws and publish privacy policies disclosing how visitor data is collected and shared. *Id.* ¶ 12; ECF 140-3 (agreement between NaviStone and Moosejaw). The browsing data of each of NaviStone's clients is never combined, shared, or disclosed. ECF 140-1 (1st Kavanagh Dec.) ¶ 9; ECF 140-8 (Expert Report of Greg Humphreys ("Humphreys Rep.")) ¶¶ 59, 124b; Third Declaration of Chris Ludwig ("3d Ludwig Dec.") ¶¶ 14, 16. In providing its service, NaviStone offers its clients the use of a JavaScript-based web analytics tool of the same kind that is employed on literally tens of millions of other websites to gather browsing data. *See* ECF 140-8 (Humphreys Rep.) ¶¶ 64, 110–20. Visitors are identified *only* by an anonymous ID number associated with a browser instance. ECF 140-6 (Second Declaration of Chris Ludwig ("2d Ludwig Dec.")) ¶ 28. NaviStone never shares this browsing data with anyone. ECF 140-1 (1st Kavanagh Dec.) ¶ 30.

NaviStone's Software Tool. NaviStone provided to Moosejaw a single line of JavaScript code ("OneTag") that Moosejaw installed on pages of its website, www.moosejaw.com. ECF 140-6 (2d Ludwig Dec.) ¶ 8. OneTag caused NaviStone's full JavaScript code to load when a user visited a page on Moosejaw's website, although this did not always or necessarily occur. *Id.* ¶¶ 10, 12. For example, if a user was running common ad-blocking software, the user's browser would not permit NaviStone's JavaScript to load or run. *Id.* ¶ 12; ECF 140-8 (Humphreys Rep.) ¶ 17. Moosejaw was solely responsible for installing OneTag on its web pages, and could remove it at any time. ECF 140-6 (2d Ludwig Dec.) ¶ 9.

The Transmittal of Clickstream Data. If the user's browser *did* permit the NaviStone code to load and run, it would send clickstream data directly to NaviStone like any common behavior tracking or analytics engines, such as Google Analytics. ECF 140-8 (Humphreys Rep.) ¶ 64. In NaviStone's case, each visitor was assigned an anonymous identifier, associated with a cookie bearing the prefix "MGX," which would be saved by the visitor's web browser. ECF 140-6 (2d Ludwig Dec.) ¶¶ 16, 27; ECF 140-8 (Humphreys Rep.) ¶ 17.3. If an MGX cookie was not saved by the browser, NaviStone could not link a visitor's different visits to the Moosejaw website

because each time a page bearing its JavaScript loaded, NaviStone would interpret this load as a new and different visitor. ECF 140-6 (2d Ludwig Dec.) ¶ 26.[2] An element of the JavaScript-based clickstream data transmittal is the use of "event handlers." ECF 140-8 (Humphreys Rep.) ¶¶ 36–37, 89. An event handler sends a signal to NaviStone if certain events occur on the webpage. *Id.* ¶ 89. For example, an event handler is able to send a signal to NaviStone when a user has entered data in a "form field" and then "tabbed out" of that field, but has not clicked "submit." *Id.* ¶¶ 81–82. Prior to June 20, 2017, *i.e.*, before the visit at issue in this case, this tab out would result in the contents typed into that form field being sent to NaviStone; after June 20, 2017, this practice ceased and only a "1" or a "0" was relayed, indicating the presence or absence of information, but not its content. *Id.* ¶ 103e(i). On a Moosejaw product page, the only event handler is linked to the "add to cart" button. *Id.* ¶ 89.

If the NaviStone code operated during a web browsing session on the Moosejaw website, the information NaviStone received was sent as a *direct* communication from the web browser to NaviStone. *Id.* ¶¶ 15–16, 103f. NaviStone did not receive the content (or a copy) of any communication between the user and Moosejaw, or in any way have access to any such communication "in transit." *Id.* ¶ 71. Rather, NaviStone received certain limited clickstream data directly from the web browsing software. *Id.* ¶¶ 15–16, 71, 103f.

Cookie Syncing. Separate and apart from the collection and transmittal of clickstream data, NaviStone's JavaScript—again, if user settings permitted it to load and operate—caused a "cookie sync" to occur. *Id.* ¶¶ 53–57. To do so, the JavaScript made a request to a third-party server hosted by a data broker called Neustar Information Services, Inc. ("Neustar"), which maintained a list of mailing addresses. *Id.* at ¶ 56; Declaration of Michael Schoen ("Schoen Dec.") ¶ 6. Upon receiving this "call out," Neustar's servers determined whether Neustar had previously

[2]The MGX cookie is a first-party cookie that expires after one year; if the user's browser permits its installation, it will remain on that browser for one year, unless the user manually deletes it. ECF 140-6 (2d Ludwig Dec.) ¶ 16.

placed a cookie from the AGKN.com domain on the user's browser instance, and, if so, whether Neustar possessed in its database a marketable mailing address Neustar associated with its cookie. ECF 140-8 (Humphreys Rep.) ¶ 56; Schoen Dec. ¶ 7. Neustar then sent back a numerical value indicating a yes-or-no whether it had an associated address. *Id.*; ECF 140-6 (2d Ludwig Dec.) ¶ 42; Schoen Dec. ¶ 8. Neustar did *not* send back an actual name and address (which NaviStone never learned), only an indication whether it possessed one. ECF 140-6 (2d Ludwig Dec.) ¶ 42; *see also* ECF 140-8 (Humphreys Rep.) ¶¶ 56–57; Schoen Dec. ¶ 10–11.

Postcard Mailing. Each night, NaviStone's servers analyzed the data collected to determine, based on pre-set criteria, which anonymous IDs had browsing behavior suggesting receptiveness to direct mail. ECF 140-6 (2d Ludwig Dec.) ¶ 34. NaviStone then asked Neustar (via automated processes) to create a mailing list of those anonymous IDs that NaviStone had identified as likely receptive and for whom Neustar had an address. ECF 140-1 (1st Kavanagh Dec.) ¶¶ 14–20. However, NaviStone did not share the underlying browsing data with Neustar, and Neustar did not share the name and address with NaviStone. ECF 140-6 (2d Ludwig Dec.) ¶¶ 37, 39; ECF 140-1 (1st Kavanagh Dec.) ¶ 14; Schoen Dec. ¶ 12. Instead, Neustar sent the mailing list directly (and solely) to American Computer Group d/b/a Computech ("Computech"), a service bureau that performed list processing. ECF 140-1 (1st Kavanagh Dec.) ¶¶ 14, 16; Schoen Dec. ¶ 10. Computech scrubbed the Neustar-provided list to remove persons who did not wish to receive postcards and then sent the scrubbed list to the printer Quad/Graphics, which printed and mailed promotional postcards. ECF 140-1 (1st Kavanagh Dec.) ¶¶ 16-18.

B. Plaintiff's Activities

Plaintiff Jeremiah Revitch is an experienced information technology professional, having worked in the industry since the 1990s. 2d DSB Dec., Ex. A (Excerpts of Deposition of Jeremiah Revitch, Vol. 1) at 17:15–18:7; 19:4–12; 27:17–19. Plaintiff also has significant familiarity with web tracking data collection and use. *See id.* at 57:17–58:21; 249:6–21; 250:7–18. His own

business runs Google Analytics on its website and has for years prior to this lawsuit. *Id*. at 198:18–23. He personally reviewed the data returned by Google Analytics for that website. *Id*.

Revitch "absolutely" visited Gizmodo's website, where articles about NaviStone were published in June 2017, before filing this lawsuit, and he was a regular reader of that site. *Id.* at 227:11–13; 310:17–21. He knows what website cookies are and what they do. 2d DSB Dec., Ex. B (Excerpts of Deposition of Jeremiah Revitch, Vol. 2) at 5:5–17. He has used private browsing to defeat tracking. 2d DSB Dec., Ex. A at 39:14–40:25. He was aware that the three browsers he has used "all have incognito or private browsing" which "prevents all kinds of cookies and – you, know, doesn't retain a history." *Id*. at 40:13–19. Revitch was aware that a privacy policy is the place to learn what a website does with a visitor's "click data." *Id*. at 43:3–12. However, his practice was not to read them because he would be "too busy reading their privacy policy," which would "severely inhibit my ability to be a retail customer of many of them ...," *id.* at 43:13–25; 115:3–7, and because he was afraid of what they might say. *Id*. at 307:16–19. He testified that even though some policies are short and readable, he does not care, because he personally does not trust privacy policies. *Id*. at 115:8–18 ("Q: I mean, privacy policies are like one or two pages. Is it really that hard – to review one to see how they treat data or how they collect data? A: I – I guess also knowing – knowing who the privacy policies are written by, I don't – I don't put a whole lot of faith in the privacy policies themselves."). He had not read a privacy policy in the last five years, apart from reading Moosejaw's policy in connection with this case. *Id*. at 44:8–13.

In March 2017, Plaintiff registered with the Moosejaw website, voluntarily providing Moosejaw with his name and mailing address. ECF 142-14 (Declaration of Kelli Patterson) ¶¶ 5, 9; ECF 142-16 (Exhibit 2 to Patterson Dec.). Plaintiff's last visit to Moosejaw.com prior to learning of NaviStone's operation was on December 8, 2017. ECF 140-24 (Plaintiff's browsing records) at 1. This was his only visit within the limitations period, as it took him nearly a year to

file this suit (which he did on November 9, 2018). ECF 1.[3] He testified that he has not deleted his cookies or browsing history associated with those visits. 2d DSB Dec., Ex. A at 105:19–106:14, 174:5–9.

In December 2017, after communicating with his lawyers, he cloned his hard drive and made a screen shot of his Moosejaw browsing history. *Id*. at 98:22–99:2; 174:13–23. This screenshot, as well as several spreadsheets recovered from his cloned drive, contained the records of his cookies and internet history, but did not contain any cookies on any browser with the prefix "MGX." *See* ECF 140-24 (Plaintiff's browsing records). After a subsequent request, Plaintiff's counsel confirmed that Plaintiff's hard drive had been searched for cookies bearing the prefix MGX, and none had been located. ECF 140-23 at 6. Had the NaviStone code run on Revitch's web browser during his visits to the Moosejaw website, it would have set an MGX cookie, unless Revitch had blocked the setting of first-party cookies.[4] ECF 140-8 (Humphreys Rep.) ¶¶ 17, 93.

[3] "Under the CIPA, the statute of limitations is one year." *Brodsky v. Apple, Inc.*, 445 F. Supp. 3d 110, 134 (N.D. Cal. 2020). Separate, recurring alleged violations trigger their own limitations periods. *Aryeh v. Canon Business Solutions, Inc.*, 55 Cal. 4th 1185, 1198–99 (2013); *Brown v. Google LLC*, 2021 WL 949372, *12 (N.D. Cal. Mar. 12, 2021); *see also Bliss v. CoreCivic, Inc.*, 978 F.3d 1144, 1148 (9th Cir. 2020) (federal wiretap act). Furthermore, Revitch cannot rely on the delayed discovery rule because he did not allege specific facts in his SAC establishing its applicability, nor can he show them here. *Nguyen v. Nissan N. Am., Inc.*, 2020 WL 5517261, *8 (N.D. Cal. Sep. 13, 2020); *Franklin v. Ocwen Loan Servicing, LLC*, 2018 WL 5923450, at *3 (N.D. Cal. Nov. 13, 2018) (to invoke the delayed discovery rule, a party "must specifically plead facts to show (1) the time and manner of discovery *and* (2) the inability to have made earlier discovery despite reasonable diligence") (emphasis in original). Even if Revitch's pleading failures were overlooked, the conduct at issue was widely publicized in a "leading tech news website," which Revitch regularly read, on June 20, 2017. ECF 43 ¶ 22; *see Shively v. Bozanich*, 31 Cal. 4th 1230, 1248 (2003) (publication can vitiate discovery rule). Moreover, he also testified—repeatedly—that, to this day, he scrupulously avoids reading privacy disclosures, which in this case would have put him on notice of the type of activity at issue.

[4]Revitch also had no recollection of receiving a Moosejaw promotional postcard within days or even weeks of his last visit to the website—or ever. 2nd DSB Dec., Ex. A at 83:23–84:3. Postcards sent in connection with the NaviStone service are triggered by browsing that occurs the business day before their mailing. *See* ECF 140-6 (2d Ludwig Dec.) ¶ 39; ECF 168 at 4 (admitting postcards sent the next day). Any mailing associated with a visit to the Moosejaw website on Friday, December 8, 2017 would have occurred on or about Monday, December 11, 2017.

III. ARGUMENT

A. Legal Standard

Summary judgment is appropriate where there is no dispute of material fact and the movant is entitled to judgment as a matter of law. Fed. R. Civ. P. 56(a).

B. NaviStone is Entitled to Summary Judgment on Plaintiff's CIPA Claims.

1. Applicable Law

Cal. Penal Code § 631(a) prohibits entities from "read[ing], or attempt[ing] to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable." California courts emphasize that an "unauthorized connection" to the transmission of information is a *requirement* of § 631, and use this point to distinguish between wiretapping (§ 631) and eavesdropping (§ 632). *See, e.g.*, *People v. Guzman*, 11 Cal. App. 5th 184, 192 (2017), *aff'd*, 8 Cal. 5th 673 (2019); *People v. Ratekin*, 212 Cal. App. 3d 1165, 1168 (1989).

Cal Penal Code § 635 prohibits the furnishing of "any device which is primarily or exclusively designed or intended for eavesdropping upon the communication of another."

2. Plaintiff Lacks Standing.

In a prior order, the Court determined that Revitch's allegations were sufficient to demonstrate standing, specifically pointing to allegations of eavesdropping and hard-drive scanning. ECF 64 at 1. But "[a] basis for standing must persist at all stages of litigation." *Zelaya v. Foot Locker*, 2018 WL 2463624, *3 (N.D. Cal. June 1, 2018) (citing *Hollingsworth v. Perry*, 570 U.S. 693, 705 (2013)). An injury sufficient to support standing must affect a plaintiff in a "personal and individual way." *Hollingsworth*, 570 U.S. at 705. The fully developed factual record rebuts Revitch's allegations of hard-drive scanning on which the Court previously relied. Scanning

did not occur here, *see* ECF 140-8 (Humphreys Rep.) ¶¶ 125–29, and Plaintiff makes no effort to argue otherwise.

As for eavesdropping, the specific facts undermine any claim of injury. NaviStone takes numerous steps to ensure that it never learns the identity of website visitors, and there is no evidence it learned Revitch's identity before he filed suit. If Revitch did not delete first party cookies, then the absence of an MGX cookie is consistent with NaviStone's code never running during his visits. *Id*. ¶¶ 17, 93, 99–100. Moreover, because Revitch had no MGX cookie, each of his visits to Moosejaw.com would appear to NaviStone as if it had been from a new user with a new anonymous ID. ECF 140-6 (2d Ludwig Dec.) ¶ 28. All NaviStone could have learned about Revitch's activity is that an anonymous *someone*—whom it could not have identified as Revitch, or even as a previous visitor to Moosejaw.com—visited a ski glove page on December 8, 2017. That is not a personal and individual injury to Revitch. Revitch's statutory standing to bring a CIPA action is anchored in § 637.2(a), which only applies to persons who "ha[ve] been injured by a violation of this chapter." While this does not require actual damages, it does require injury. As there is no possibility—let alone evidence—that NaviStone associated the single page visit at issue here (or any others) with Revitch, there is no injury.

3. Plaintiff Consented to NaviStone's and Moosejaw's Actions.

Lack of consent is an element of Revitch's proof of wiretapping under § 631. *See In re Google Assistant Privacy Litig.*, 457 F. Supp. 3d 797, 828 (N.D. Cal. 2020); *see also Reyes v. Educ. Credit Mgmt. Corp.*, 773 F. App'x 989, 990 n.1 (9th Cir. 2019).[5] Consent may be implied from the surrounding circumstances. *In re Google, Inc. Gmail Litig.*, 2014 WL 1102660, *16 (N.D. Cal. Mar. 18, 2014); *cf. Com. v. Proetto*, 771 A.2d 823, 831 (Pa. Super 2001) (implied consent to recording of internet communications presumed under Pennsylvania's two-party consent wiretapping statute).

[5]On this undisputed factual record, the same result would obtain were the Court to treat consent as an affirmative defense.

Behavioral analytics software is ubiquitous. ECF 140-8 (Humphreys Rep.) ¶¶ 109–16. The vast majority of Americans are aware of internet data tracking and its use to create targeted advertising. *See* ECF 140-25 (Pew Research Center Report) at 3, 6–8. Critically, as noted earlier, Revitch has, since at least 2016, used behavioral tracking *on the website of his own business*. ECF 140-8 (Humphreys Rep.) ¶ 118. He is an experienced IT professional who knows how websites generate user-specific advertising and who is knowledgeable of web infrastructure and privacy measures (ad blocking and cookie blocking) generally. 2d DSB Dec., Ex. A at 57:17–58:21, 249:6–21, 250:7–18. He knows that to determine how a website handles user data, one should look at the privacy policy, yet he refuses to do so. *Id*. 43:3–12.[6]

Revitch opined that data sharing practices "shouldn't be buried in a privacy policy." *Id*. at 320:16–321:4. His preference is not the law. California has a statute dictating how data collection and sharing practices should be disclosed, *see* Cal. Bus. & Prof. Code § 22575 *et seq*., and Moosejaw's disclosures complied with that law. Revitch's refusal to take advantage of that statutorily-mandated disclosure—despite asserting that "statutes in place help ensure my privacy," 2d DSB Dec., Ex. A at 49:1–7—cannot be laid at NaviStone's feet. Revitch's behavior created implied consent, and he cannot use willful blindness to avoid this conclusion.

4. NaviStone Acted as an Extension of Moosejaw.

At all times, NaviStone acted as a vendor and service provider for Moosejaw, rendering it an extension of Moosejaw itself, a fact with which Revitch agrees. *See* ECF 168 at 2 & 10. Only Moosejaw, not NaviStone, had the ability and authority to install or uninstall OneTag on the

[6]Nor can such behavior be written off as pre-litigation ignorance, subsequently corrected. Revitch visited two online retailers the day before his deposition, 2nd DSB Dec., Ex. A at 54:24–55:3, but did not read the privacy policy of either, *id*. 43:3–12, 56:6–16, 57:10–16, nor did he otherwise make any efforts to learn of their data practices. Had he done so, he would have learned that www.jensonusa.com is currently running 16 different pieces of analytics and tracking software and www.backcountry.com is running 7. This information is publicly available using www.builtwith.com, a web utility that enables users to freely analyze what different technologies are used to build different web pages.

Moosejaw website. ECF 140-6 (2d Ludwig Dec.) ¶ 9. When NaviStone both received browsing data and analyzed it, it acted exclusively as an agent for Moosejaw. ECF 140-1 (1st Kavanagh Dec.) ¶ 10; 2d Kavanagh Dec. ¶ 5. By contract, it could not sell or share the data it received from visitors to its client websites; and, unlike other services, such as Google Analytics, it did not and does not engage in any cross-site analysis or profiling (combining data collected on different client sites to build profiles of individual users). ECF 140-1 (1st Kavanagh Dec.) ¶ 10, 13; ECF 140-3 (contract between NaviStone and Moosejaw) at 2; 3d Ludwig Dec. ¶¶ 14–16. NaviStone only used data it received from Moosejaw site visitors to benefit Moosejaw and all its actions pertinent to this case were taken strictly for and on behalf of Moosejaw. ECF 140-1 (1st Kavanagh Dec.) ¶ 10; 2d Kavanagh Dec. ¶ 5.

A court in this district recently considered—and dismissed—allegations under § 631 against several other companies that provide similar behavioral analytics services. *See Graham v. Noom, Inc.*, 2021 WL 1312765 (N.D. Cal. Apr. 8, 2021); *Yale v. Clicktale, Inc.*, 2021 WL 1428400 (N.D. Cal. Apr. 15, 2020). The court in *Graham* found that, while the defendant FullStory's code did transmit visitor data to its servers, it acted as a vendor and that "as a service provider, FullStory is an extension of Noom." *Id.*

The *Graham* court distinguished this Court's order denying in part NaviStone's motion to dismiss, but did so relying on allegations contained in Revitch's complaint that are false. For example, it noted that, *as alleged* in this case, NaviStone was "an online marketing company and data broker that deals in U.S. consumer data" and that NaviStone had "captured the data, de-anonymized it, and matched it with other databases, thereby creating marketing databases of identified website visitors;" that NaviStone "partnered with e-commerce sites to intercept visitor data and create marketing databases of consumer information;" and that NaviStone "mined information from other websites and sold it." *Id.* None of this is true.

On summary judgment the *facts* discovered, not the *allegations* made, are what matters. While NaviStone receives certain clickstream data from its client's websites, it does not sell or share that data with anyone. NaviStone uses such data "solely to perform its obligations pursuant to this Agreement or pursuant to any other written agreement with Client. NaviStone shall not disclose Client Data to any third party except as reasonably required for NaviStone to provide its obligations under the Agreement or as required by law or court order." ECF 140-3 (contract between NaviStone and Moosejaw) at 2. Browsing data is segregated and not combined with any information about other retailers and their websites. ECF 140-1 (1st Kavanagh Dec.) ¶ 28; 3d Ludwig Dec. ¶ 16. Nor does NaviStone use data obtained in connection with its work for one client in its work for any other client. *Id*. The data it collects is not available for sale or use by any party other than the client for which it was collected, and NaviStone does not "create marketing databases" for its own clients, let alone anyone else. ECF 140-1 (1st Kavanagh Dec.) ¶¶ 28–30.

Notably, had Moosejaw simply hired software engineers as employees to write code for its website that accomplished *exactly* what NaviStone's code does, Moosejaw could not have been liable, because as the Court has already found, a party to a communication cannot wiretap itself in violation of § 631. ECF 64 at 4. It makes no sense to assign liability where the effect on the web user is exactly the same, simply because the result is accomplished by a contractor working for Moosejaw's sole benefit rather than Moosejaw employees themselves. Moreover, here, the use of a contractor helped protect visitor anonymity. ECF 140-8 (Humphreys Rep.) ¶¶ 50–52; ECF 140-7 (First Declaration of Greg Humphreys) ¶ 6.

Holding service providers to be equivalent to parties preserves the principle, articulated in *Starbuck Corp. v. Superior Court*, that "a statute is to be construed in such a way as to render it reasonable, fair and harmonious with its manifest legislative purposes, and the literal meaning of its words must give way to avoid harsh results and mischievous or absurd consequences." 168 Cal. App. 4th 1436, 1449 (2008) (cleaned up). A narrow construction is all the more important when

construing a penal statute. *See id.* at 1450. Revitch's contrary view would lead to the conclusion that any third-party analytics service provider, and any site on which that provider's code runs, commits criminal offenses innumerable times after a visitor loads a webpage. This would ensnare tens of millions of web pages that are visited every single day. And it would provide no benefit to California web users, since the exact same activity is unquestionably legal if accomplished by the website operator itself, rather than a contractor acting as the operator's agent. The Court can avoid this absurd result by holding that a website operator's agent is, for CIPA purposes, standing in the website operator's shoes.

5. NaviStone Did Not Acquire Information "In Transit," Nor Did It Make an Unauthorized Connection to a Transmission Line.

Even if the NaviStone code ran and there were communications from Revitch's browser instance to NaviStone, those communications were entirely distinct from and different than any communications to or from Moosejaw, and so were not acquired while "in transit" as required by § 631.

When a visitor entered the URL of a page on the Moosejaw website into their browser's address bar, their browser requested page elements from Moosejaw's server and various third-party servers and loaded the page. Only after the page was fully loaded did the NaviStone-provided JavaScript begin to run. ECF 140-8 (Humphreys Rep.) ¶¶ 15–16, 41a–b, 68, 70–71, 103, 107. And the communications sent from Revitch's web browser to NaviStone were wholly distinct from those sent between Revitch's browser and Moosejaw. *Id*. While they may have been *related* to the same browsing activity, they were not identical, and there is no evidence that NaviStone's code copied, or even had access to, communications between Revitch and Moosejaw. *Id*. ¶ 70–71. Indeed, all of the evidence in this case, and the testimony of the experts, is to the contrary.

That distinguishes this case from *In re Facebook, Inc. Internet Tracking Litigation*, 956 F.3d 589 (9th Cir. 2020).[7] *Facebook*—decided at the pleading stage—dealt with an allegation that Facebook had *duplicated* web user's GET requests and forwarded those duplicates to itself. *Id.* at 608. Here, as the record shows, the communications sent to NaviStone were not duplicates of those sent to Moosejaw. Second Declaration of Greg Humphreys ¶¶ 3–8; 3d Ludwig Dec. ¶¶ 9–11. Indeed, at times, no communication was sent to Moosejaw *at all*. For example, when a user typed information into a form field and "tabbed out" of it, no information had yet been sent to Moosejaw. ECF 140-8 (Humphreys Rep.) ¶ 68. NaviStone received a direct communication indicating that information had been typed in the field, but it did not receive the contents of the field.[8] *Id.* ¶ 103e. Similarly, placing an item in the shopping cart triggered one distinct command to Moosejaw's servers (instructing them to place a specific item in the user's shopping cart) and to NaviStone (informing it only that the add-to-cart button has been clicked). *Id.* ¶ 41b.

In short, the communications to NaviStone were independent, took place after communications to Moosejaw, and did not duplicate them, as was alleged in *Facebook*. As a result, it cannot be said that NaviStone was "reading" the "contents or meaning" of any communications to Moosejaw while they were "in transit," as required by § 631.

Moreover, the California courts have made clear that § 631 and § 632 cover different activities, with § 632 focused on "eavesdropping," or listening in on confidential communications, and § 631 focused on "wiretapping," or making an unauthorized connection to a transmission line. *See, e.g., Guzman*, 11 Cal. App. 5th at 192 ("Section 631 prohibits ... intercepting communications

[7]This case differs from *Facebook* in another vital way. In that case, the plaintiff alleged that the defendant had used this duplicated information to learn information in a way it had expressly told users it would not do. Here, Moosejaw's privacy policy put users on clear notice of the potential uses of information being gathered and shared.

[8]To analogize to physical space: when an individual places a letter in a mailbox, she communicates two things. First, she sends a communication to the recipient of the letter, *i.e.*, its contents. Second, she communicates (through her action) to anyone observing her the fact that she has sent a letter. She may, for example, raise the flag on her mailbox to signal the presence of outgoing mail. These are distinct communications. Someone who sees the raised flag has not thereby read the letter.

by an unauthorized *connection* to the transmission line.") (emphasis in original) (quoting *Ratekin*, 212 Cal. App. 3d at 1168). There is *no* transmission line connection here. Moreover, Moosejaw itself installed—and thus authorized—the code that sent information directly to NaviStone.

6. NaviStone Did Not Intercept Any "Contents" of Communications.

A violation under § 631 also requires acquisition of the "contents" of communications. In denying NaviStone's motion to dismiss, the Court found that as alleged, Revitch's mouse clicks were "communications." *See* ECF 64 at 3. The summary judgment record shows that during the only visit within the limitations period, Revitch viewed a single product page. NaviStone could only have learned from that action that an anonymous individual had loaded a webpage. The term "contents" includes only "the intended message conveyed by the communication, and does not include record information regarding the characteristics of the message that is generated in the course of the communication." *In re Zynga Privacy Litig.*, 750 F.3d 1098, 1106 (9th Cir. 2014). While a URL may constitute "contents," *id.*, at 1108–09, that is only if it contains actual terms typed by the user. Revitch offers no evidence that the single URL visited on December 8, 2017 contained any such information.

7. NaviStone Is Entitled to Summary Judgment on Plaintiff's § 635 Claim.

It strains credulity to suggest that behavioral tracking JavaScript is "primarily" or "exclusively" designed for eavesdropping. Plaintiff's only argument to the contrary is that NaviStone's code "is designed to gather PII [personally identifying information], including keystrokes, mouse clicks, and other electronic communications." ECF 168 at 17 (brackets added). Plaintiff's only record citation in support of this claim is an allegation from his complaint, which is "not evidence that can be used to support or oppose summary judgment." *Briggs v. Blomkamp*, 70 F. Supp. 3d 1155, 1166 (N.D. Cal. 2014) (citations omitted). The banal assertion that NaviStone's JavaScript gathers data is unhelpful; all JavaScript behavioral tracking software gathers data, including that used by Plaintiff, Plaintiff's counsel, Plaintiff's experts, and many

government entities. Data-gathering software is not *per se* primarily or exclusively designed for eavesdropping (in violation of § 632) or wiretapping (in violation of § 631).

In addition, Plaintiff's § 635 claim fails because it must fall with his § 631 claim. A CIPA civil action requires injury. Cal. Penal Code § 637.2. One cannot be injured by the "furnishing" of a device for eavesdropping without being a victim of said eavesdropping. No actionable eavesdropping occurred here, so there is no injury that could support § 637.2 standing to bring—let alone, prove—a § 635 violation.

8. Revitch Is Not Entitled to Statutory Damages.

Courts in this district have recognized that where a plaintiff suffers no actual harm, an award of statutory damages may be unconstitutionally excessive. *See Campbell v. Facebook, Inc.*, 315 F.R.D. 250, 268–69 (N.D. Cal. 2016). For much the same reason Revitch's lack of actual injury deprives him of standing, so too it shows that an award of $5,000 would plainly be excessive for conduct that could not have allowed, and did not allow, NaviStone to associate any browsing activity with Revitch.

C. NaviStone is Entitled to Summary Judgment on Plaintiff's Common Law Claims.

Revitch alleged common law and California constitutional claims of invasion of privacy. *See* ECF 43, ¶¶ 92-106. They survived motions to dismiss because the Court determined that allegations "that NaviStone's code scanned Revitch's computer for files that revealed his identity and browsing habits" might constitute the required "highly offensive breach of norms." ECF 64 at 6. On the factual record here, the Court should enter judgment for NaviStone.

First, Revitch abandoned these claims. He did not attempt to certify them. *See generally* ECF 134. He informed the Court he was "prepared to move for summary judgment on his claims against NaviStone and on NaviStone's counterclaim." ECF 160 at 1, ¶ 3. Given that opportunity, *see* ECF 166, he chose not to argue them. NaviStone is entitled to summary judgment on these abandoned claims. *See Brach v. Newsom*, 2020 WL 7222103, *10 (N.D. Cal. Dec. 1, 2020).

Second, the facts do not support them. Revitch would have to demonstrate "a highly offensive breach of norms." ECF 64 at 6 (citing *In re Facebook, Inc. Consumer Privacy User Profile Litig.*, 2019 WL 4261048, *17 (N.D. Cal. Sept. 9, 2019); *see also id*. at 5. While Revitch repeatedly *alleged* that NaviStone scanned his hard drive to learn his identity, *see* ECF 43, ¶¶ 1-3, 9, 17, 20, 26, 42-46, 86, that did not happen. ECF 140-8 (Humphreys Rep.) ¶¶ 125–29. NaviStone never scanned any hardware, and never learned Revitch's identity. The only conduct Revitch *can* identify NaviStone engaging in is routine and ubiquitous behavior tracking on behalf of Moosejaw on the Moosejaw website only. Revitch has not even attempted to show he suffered actual harm from such conduct. *See* ECF 168 at 8-9 (seeking only CIPA statutory damages).

D. NaviStone is Entitled to Summary Judgment on Its Counterclaim for Declaratory Relief.

NaviStone seeks a declaration that (1) Moosejaw's privacy policy adequately discloses the data collection at issue here; (2) Moosejaw's privacy policy meets the requirements for commercial privacy policies set out in California law; and, on these facts, (3) CIPA should be construed not to criminalize the conduct alleged here. Such a declaration would harmonize CIPA with California's Internet privacy laws, provide certainty to e-commerce businesses, and comport with the clear intent of the state legislature.

CIPA was originally passed in 1967. Rather than amending CIPA to address the rise of the Internet, *cf. Smith v. LoanMe, Inc.*, 2021 WL 1217873, *6–7 (Cal. Apr. 1, 2021) (discussing CIPA amendment applying to cell phones), California has adopted numerous separate statutes *explicitly aimed* at protecting online privacy: the Privacy Rights for California Minors in a Digital World Act, Cal. Bus. & Prof. Code § 22580 *et seq.*; Shine the Light Act, Cal. Civ. Code § 1798.80 *et seq.*; and the California Consumer Privacy Act ("CCPA"), Cal. Civ. Code § 1798.100 *et seq*., recently amended by the California Privacy Rights Act ("CPRA"), 2d DSB Dec., Ex. C. Most relevant to this dispute is the 2003 California Online Privacy Protection Act (CalOPPA). CalOPPA requires "operator[s] of commercial Web site[s]" that collect personally identifying information (PII) or

provide such information to third parties to "conspicuously post" a privacy policy on their websites. Cal. Bus. & Prof. Code § 22575. The term "conspicuously post" is defined, and a website satisfies the requirement if it includes a text link on its homepage to the privacy policy that includes the word "privacy." Cal Bus. & Prof. Code § 22577(b)(3)(A).

When CalOPPA was passed in 2003, the accompanying California Senate analysis noted that "existing law does not directly regulate the privacy practices of online business entities." Sen. Rules Com., Off. Of Sen. Floor Analyses, 3d reading analysis of Assem. Bill No. 68 (2003–04 Reg. Sess.). Existing law included CIPA, a criminal statute then on the books for 36 years. Notably, CalOPPA demonstrated the legislature's policy choice to adopt a disclosure regime, as opposed to restrictions on data collection and transmittal to third parties. As the bill's author said, the disclosure model would "provide [] meaningful privacy protection [] that will help foster the continued growth of the internet economy." Assem. Com. on Bus. and Prof., Analysis of Assem. Bill No. 68 (2003–2004 Reg. Sess.). The California Supreme Court has taken these comments seriously, writing that "[t]he enactment of [CalOPPA] suggests that when the Legislature intends to address online transactions, it does so unambiguously. In addition, the fact that C[al]OPPA enacts merely a disclosure regime suggests that the Legislature in 2003 sought to proceed cautiously in regulating online commerce." *Apple Inc. v. Superior Court*, 56 Cal. 4th 128, 148 (2013). CalOPPA's passage demonstrates that California's legislative vision for online privacy is based on disclosure.

Nor was that the end of the matter. In 2013, the legislature amended CalOPPA, specifically in response to the rise of behavioral tracking on websites. The author of the amendment stated:

> Since the California Online Privacy Protection Act (CalOPPA) took effect … online commerce has burgeoned and evolving technology and new business practices have raised new privacy concerns. One practice that raises privacy concerns is online tracking, also called online behavioral tracking. This is the monitoring of an individual across multiple websites to build a profile of behavior and interests. In the age of smart phones and tablets, similar tracking is also done by monitoring individuals as they use different apps and different phone features. The resulting profiles are commonly used to deliver targeted advertisements.

Sen. Comm. on Bus., Prof., & Econ. Dev., Committee Report, Bill Analysis to AB 370. The same committee report also noted that the average visit to a web page triggered 56 instances of data collection. *Id*.

In response to concerns over behavioral tracking specifically, the legislature did not restrict or prohibit the practice. Instead, it increased the disclosure requirements, requiring commercial website operators to (1) disclose how they respond to "do not track" requests; and (2) disclose whether other parties may collect personally identifiable information about an individual consumer's online activities over time and across different web sites when using the operator's web site or service. Cal. Bus. Prof. Code § 22575(b)(5)–(6).

California has continued to refine its regulation of behavioral tracking online. In 2018, California passed the CCPA (eff., Jan. 1, 2020), which granted new rights to consumers concerning data collection, including the right to know what information is collected and how it is used and shared; the right to delete personal information; and the right to opt-out of the sale of PII; it also imposed related notice obligations for website privacy policies. Again, nothing in the CCPA prohibits data collection or online behavioral tracking; it simply increases consumer transparency surrounding it and provides rights to know or delete information previously collected. The CCPA was amended in 2020 with the passage by ballot initiative of the CPRA. The "findings" section of the CPRA acknowledged that California is a leader in new technologies, that internet businesses have had great success by relying on advertising rather than consumer sales, and that much of this business was reliant on consumer data tracking. As before, the CPRA does not prohibit such practices, but simply provides—yet again—for enhanced disclosures. CPRA expressly recognizes that businesses may share consumer data with service providers and contractors. *See* 2d DSB Dec., Ex. C (CPRA ballot initiative full text) § 4.

This body of regulation, and its history, reveals certain critical facts. *First*, California's legislature—and its citizens acting in a legislative capacity—are well aware that behavioral

tracking exists and that internet browsing has the capacity to generate large amounts of data which may be recorded, shared, and sold. *Second*, California does not prohibit this data collection or sharing, recognizing that it forms a backbone of e-commerce. Instead, it permits behavior tracking and data collection subject to an increasingly stringent disclosure regime so that Californians may understand what data is collected from them and how it is used.

The application of these principles reveals the flaws in Revitch's claims. NaviStone is a service provider. It assists its clients, in this case Moosejaw, with their marketing practices by analyzing their website traffic and utilizing external partners to enable Moosejaw to mail special offers to individuals likely to be interested. This is exactly the type of information-sharing that CalOPPA and its successors addressed, and none of those statutes criminalizes such sharing. Instead, they mandate that it be disclosed—as Moosejaw did here.

The privacy policy Moosejaw had in place at the time of Revitch's browsing made several disclosures that cover the conduct at issue in this case. It disclosed that Moosejaw would share information collected from users with third parties in order "to help us personalize our service offerings, website, and advertising" and "to send you information about our products, services, and promotions." ECF 25-2 (Moosejaw Privacy Policy) at 2. It also disclosed that "we share Information with service providers that help with our business activities, including shipping vendors, billing and refund vendors, payment card processors, and companies that help us improve our products and services." *Id*. at 3. It stated, "Moosejaw may share your information with other companies in order to provide you with a special offer or promotion that we think you will find valuable. Unless you specifically tell us that you do not want to receive these special offers (we can't imagine why), we may share your Information." *Id*.

This language describes what NaviStone did for Moosejaw. The data sharing enabled by NaviStone's software helped Moosejaw personalize its offerings and advertising. NaviStone is a service provider whose work enabled Moosejaw to improve its products and services by targeting

appropriate products to users likely to be interested. The use of NaviStone's services to enable the mailing of postcard offers was "to provide [customers] with a special offer or promotion that we think [customers] will find valuable." No reasonable reader could view this policy, learn about NaviStone's services, and conclude that those services had not been disclosed.

This law and these facts frame the issue: the California law of internet data sharing is based on disclosure *via* a privacy policy. Moosejaw has a privacy policy that complies with that law. That policy fairly discloses the type of activity at issue in this case: the sharing of visitor data with third-party service providers for the purpose of enabling marketing and promotions. On those facts, the disclosed activities cannot and should not be deemed to violate CIPA. Holding that disclosed data collection, though compliant with statutes governing data collection, nonetheless constitutes a criminal violation of CIPA would disrupt the legislative scheme that regulates internet privacy.

Revitch raises a number of unpersuasive arguments why NaviStone's counterclaim should fail.

First, Revitch claims that because NaviStone made this argument in its motions to dismiss, and because the motions to dismiss were not granted (in full), the Court has decided this issue, making it the "law of the case." ECF 168 at 12. This theory, copied and pasted from Plaintiff's Motion to Dismiss NaviStone's Counterclaim (ECF 76 at 5–7), which was denied, borders on frivolous. In partially denying NaviStone's motions to dismiss, the Court said nothing about the CalOPPA argument. When Revitch argued previously that this denial constituted a ruling on the merits of the CalOPPA argument, the Court rejected this argument in a one-sentence order. *See* ECF 82. Furthermore, there is now a factual record providing a basis for the Court to rule on how CalOPPA and CIPA interact. The issue is ripe for decision, not already decided.

Second, Revitch argues that NaviStone is seeking an advisory opinion because "the Moosejaw privacy policy and CalOPPA compliance is irrelevant to Plaintiff's claims." ECF 168 at 21. NaviStone is not seeking a naked declaratory judgment that Moosejaw's privacy policy

complies with CalOPPA. It seeks a more specific declaration that the Moosejaw privacy fairly discloses the type of activity in which NaviStone engages, and that, because of this disclosure, Revitch's CIPA claims fail. A ruling for NaviStone would require judgment in its favor, and is therefore not an advisory opinion.

Revitch suggests that his self-imposed ignorance of the privacy policy renders any opinion of this Court advisory, preemptively arguing that NaviStone will speculate that he read it. NaviStone takes Revitch at his word that he did not read this policy, and in fact purposefully chooses not to review *any* privacy policies, despite knowing what they are and why they exist. That admission is not harmful to NaviStone's counterclaim, but fatal to Revitch's case. It negates the essential element of non-consent. CalOPPA provides a vehicle for consent—privacy policies—but does not require anything further (such as pop-up windows or checkboxes). Revitch, an experienced technology professional familiar with the reason for privacy policies and the underlying technology at issue, should be presumed to have consented to the activities such policies disclose. To hold otherwise would render the CalOPPA disclosure regime superfluous and capable of destruction by willful ignorance.

Third, Revitch argues that Moosejaw's privacy policy "contains false information and is thus noncompliant." ECF 168 at 23. This argument rests on a tortured, acontextual reading. Plaintiff claims that because the privacy contains the sentence, "we only share your information with reputable companies who provide products or services that we believe interest our customers," and because NaviStone does not offer products or services directly to retail consumers, the privacy policy is false. *Id*. This "reading" ignores numerous other sections of the policy that disclose the type of activity at issue here. The quoted sentence is immediately preceded by the statement, "Moosejaw may share your Information with other companies in order to provide you with a special offer or promotion that we think you will find valuable." This describes NaviStone's role on the Moosejaw website. In addition, the policy discloses that Moosejaw shares information

"with service providers that help with our business activities." It strains credulity to argue that NaviStone is not a "service provider" that "helps with Moosejaw's business activities." NaviStone acted as an agent for Moosejaw with the sole purpose of assisting Moosejaw with its marketing.

Moreover, NaviStone's services operate in the interest of Moosejaw's customers, even if NaviStone does not directly provide services to those customers. NaviStone enables customers to receive a deal in a manner that does not cause their identity to be shared with Moosejaw unless the customers choose to take advantage of it.

Plaintiff suggests that Moosejaw breached its contract *with NaviStone* by not including what it describes as "mandatory language" provided by NaviStone in its privacy policy. ECF 168 at 23. NaviStone believes that the language Moosejaw included was sufficient—indeed, the contract does not dictate the precise language which must be used. But, even if Moosejaw's disclosure fell short of its contractual commitment in some way, that would be a dispute between NaviStone and Moosejaw. Whether Moosejaw lives up to its contractual obligations to NaviStone has no bearing on whether the disclosure satisfies CalOPPA.

Fourth, Revitch claims that conduct compliant with CalOPPA may nonetheless violate CIPA. He relies on a ruling on a motion to dismiss in *In re Google, Inc.*, 2013 WL 5423918 (N.D. Cal. Mar. 13, 2013), in which the court concluded that Google users had not consented to Google's "interception" of emails. Revitch ignores crucial context. The court analyzed the text of the policies and concluded that—based on *only* the information available at the pleading stage—they did not fairly disclose the alleged interception. The court did not rule that privacy policies are *never* relevant in assessing CIPA claims, but that, on the information in the pleadings, they did not disclose the challenged activity. Revitch's citation to *Hart v. TWC Product and Technology LLC*, 2021 WL 1032354 (N.D. Cal. Mar. 17, 2021) fares no better. That case—which involved *no* CIPA claims—was decided on the pleadings, and the court explicitly found that it lacked sufficient information concerning the presentation of the policy to determine its effect on the plaintiff's

reasonable expectation of privacy. *Id.* at 5.[9] That is not the case here. The privacy policy is in the record, and the Court can adequately evaluate its disclosures and their effect on the case.

Revitch also argues, again citing the 2013 *In re Google* case, that CIPA establishes broad privacy protections and that CIPA can apply to new technologies that did not exist at its passage. NaviStone does not quarrel with those broad propositions, but they do not lead to Revitch's preferred result. California courts have a standard method of applying old statutes to new technologies. Specifically, California courts are to "ask [themselves] how [the legislature] would have handled the problem had it anticipated it." *Ward v. Tilly's, Inc.*, 31 Cal. App. 5th 1167, 1178 (2019). That analysis is easier than usual in this case because the Court need not hypothesize what the legislature *might* have done to regulate data collection; the Court can look at what it *actually did*. CalOPPA was first passed in 2003, because the legislature found that "existing law"—which included CIPA—"does not directly regulate the privacy practices of online business entities" and that enacting a disclosure regime for online privacy would "provide meaningful privacy protection" while also "foster[ing] the growth of the internet economy." Assem. Com. on Bus. & Prof., Analysis of Assem. Bill No. 68 (2003–2004 Reg. Sess.); *see also Apple*, 56 Cal. 4th at 148 (citing same).

The legislature subsequently confronted the issue of behavioral tracking explicitly, flagging the issue and noting that "[o]ne practice that raises privacy concerns is online tracking, also called online behavioral tracking" which it described as monitoring individuals' behavior on websites to build advertising profiles and deliver targeted ads. *See* Committee Report, Bill

[9]NaviStone respectfully disagrees with one aspect of Judge Tigar's ruling—which does not bind this Court—in particular. The opinion cites *Nguyen v. Barnes & Noble, Inc.*, 763 F.3d 1171, 1178–79 (9th Cir. 2014) for the proposition that the court needed to determine whether the plaintiff was on actual or constructive notice of the policy. But *Nguyen* involved an arbitration agreement, which purported to bind users. In that case, assent to be bound—and as a corollary, constructive notice—is a critical inquiry. In the context of privacy policies that discloses a website's privacy practices, the court need not determine mutual assent because the website does not purport to bind the visitor to privacy policy terms. Conspicuousness—from which one could infer notice—is defined by statute. Revitch does not argue that the Moosejaw privacy policy is inconspicuous.

Analysis to AB 370, *supra*. The legislature addressed this issue by adding further disclosure requirements, not by restricting the use of behavioral tracking and clickstream data. Holding that disclosures and activity that are compliant with CalOPPA nonetheless violate CIPA would upset this careful balance and disregard the principle (which Revitch himself acknowledges, *see* ECF 168 at 27) that "[f]or purposes of statutory construction, the various pertinent sections of all the codes must be read together and harmonized if possible." *People v. Bustamante*, 57 Cal. App. 4th 693, 699 (1997). CIPA cannot be harmonized with CalOPPA if conduct that is properly disclosed under CalOPPA is nonetheless determined to be criminal wiretapping.

Revitch's attempts to distinguish *Apple* rely on a mischaracterization of NaviStone's position. Yes, *Apple* involved harmonizing CalOPPA with another privacy law, the Song-Beverly Act, not CIPA, but the applicable legal principle is the same: *Apple* teaches that when the California legislature wants to regulate online privacy, it does so explicitly, using a disclosure regime. *Apple*, 56 Cal. 4th at 148. *Apple* likewise teaches that it is appropriate to examine legislative history to harmonize statutes that might otherwise conflict. *Id*. Revitch asserts that nowhere in the *Apple* opinion "did the California Supreme Court find that CalOPPA would preclude all privacy-oriented consumer suits and causes of action." ECF 168 at 27. That is a strawman: NaviStone does not contend that CalOPPA displaces *all other privacy laws*. NaviStone argues that where CalOPPA is *explicitly targeted* at a certain category of conduct (the use of behavioral analytics) and provides a regulatory model (disclosure), and where the conduct in this case falls within that category and satisfies that regulatory model, then, in order to harmonize the two statutes, CIPA should not be interpreted as criminalizing that conduct. That is far from the broad prohibition Revitch has conjured up.

Fifth, Revitch makes several arguments concerning (1) whether Ohio or California law applies and (2) whether CIPA applies to "new technologies." While NaviStone believes that applying California law to an Ohio company that receives communications on servers in Virginia

poses Commerce Clause questions, NaviStone raises that issue only to preserve it, and concedes that under existing case law, California law likely applies. As to the second issue, NaviStone agrees that CIPA *can* apply to new technologies; the question is whether and how it *should*. With regard to properly disclosed behavioral tracking, CIPA should not apply, for the reasons discussed *supra*.

CIPA might well apply to behavioral tracking if it occurred in a context not covered by CalOPPA. If a hacker installed technology that tracked user behavior unbeknownst to the user and the website operator, there would be no practical way for the website operator to disclose this, so CalOPPA's disclosure regime would not be sufficiently protective. Even in cases where the site operator knew, an inadequate disclosure might give rise to CIPA liability. ***But these questions are not at issue here***. For the purposes of this motion, the Court need not decide whether CalOPPA always displaces CIPA, nor need it decide whether CalOPPA's remedies for noncompliance are exclusive of CIPA's remedies. Those issues are not before the Court because, again, Plaintiff has raised exactly *one* (non-credible) objection to the privacy policy, which is based on an acontextual, selective reading that ignores the rest of the document.[10]

IV. CONCLUSION

The undisputed facts in this case show that the JavaScript plaintiff contends to be a "wiretap" is no different from JavaScript-based behavioral analytics tools that run on millions of websites every day. Declaring these tools to be illegal "wiretaps" would be contrary to California law; would cause massive damage to the e-commerce economy; and would not be faithful to the clear regulatory scheme California has created to protect internet privacy through timely disclosures. For the foregoing reasons, the Court should deny Plaintiff's motion for summary judgment, and grant NaviStone's cross-motion for summary judgment.

[10]Revitch also claims that NaviStone is seeking an advisory opinion concerning CalOPPA's interaction with § 632 of CIPA. However, because Plaintiff's § 632 claim has been dismissed with prejudice, § 632 is not at issue and need not be addressed.

Respectfully submitted,

Dated: April 22, 2021

/s/ David Swetnam-Burland
David W. Bertoni *(pro hac vice)*
dbertoni@brannlaw.com
David Swetnam-Burland (226216)
dsb@brannlaw.com
Eamonn R.C. Hart (*pro hac vice*)
ehart@brannlaw.com
BRANN & ISAACSON
184 Main Street, 4th Floor
P.O. Box 3070
Lewiston, ME 04243-3070
Tel.: (207) 786-3566
Fax: (207) 783-9325

Richard Pachter (120069)
richard@pachterlaw.com
LAW OFFICES OF RICHARD PACHTER
555 University Avenue, Suite 200
Sacramento CA 95825
Tel.: (916) 485-1617
Fax: (916) 379-7838

Attorneys for NaviStone, Inc.